==========
H I P A A L E R T -- Volume 3, Number 10 - October 22, 2002

>>From Phoenix Health Systems--HIPAA Knowledge--HIPAA Solutions<<
=>Healthcare IT Consulting & Outsourcing<=
==========
HIPAAlert is published monthly in support of the healthcare industry's efforts to work together towards HIPAA security and privacy. Direct subscribers total over 19,000.

IF YOU LIKE HIPAAlert, YOU'LL LOVE www.HIPAAdvisory.com! -- Phoenix' "HIPAA Hub of the Web"
==========

T H I S I S S U E

==========

Join us NEXT WEEK for...

"HANDS-ON-HIPAA: Testing Your Transactions and Code Sets" AudioConference.

On Tues., Oct. 29 at 2 PM Eastern, Phoenix Health Systems' Principal Linda Ostach provides guidance and practical advice for proceeding with the next phase of testing your electronic transactions for HIPAA.

To sign up or for more info, go to our HIPAAstore: http://www.hipaadvisory.com/ezcart/

==========

1 >> F R O M T H E E D I T O R S:

With just six months remaining until the April 2003 deadline for HIPAA Privacy compliance and readiness for Transactions testing, this issue of HIPAAlert marks a significant psychological, if not official, HIPAA milestone for many of us. There are no regulatory reprieves pending, nor influential suits, nor promising attempts for legislative dilution of the regulations. HIPAA Privacy and Transactions standardization is with us, like it or not. HIPAA Security Rules? We are told to expect the final version this year, but -- no matter -- security measures come with the territory and cannot be ignored, with or without final official verbiage.

This issue follows suit: the focus is on HIPAA implementation. Offerings range from an authoritative tutorial on the often missed -- and misunderstood -- issue of HIPAA as it applies to employee health benefit plans (by policy experts Bill and Lisa MacBain), to an update on the soon-to-be-finalized Transactions Addenda (by HIPAA EDI guru Kepa Zubeldia), to a legal analysis of the recent HHS Privacy FAQ (by attorneys Steve Fox and Rachel Wilson), to another entertaining Helen Hadley illustration of HIPAA reality in her before-and-after "play" on HIPAA in a typical medical practice. Lest we forget techonology's role in HIPAA, security expert

Eric Maiwald reminds us of the value and need for appropriate encryption to protect confidential communications.

D'Arcy Guerin Gue, Publisher
dgue@phoenixhealth.com

Bruce Hall,
Director of Internet Services
bhall@phoenixhealth.com

==========

2 >> H I P A A n e w s

** CMS Busy with Transactions Enforcement, Compliance Extensions, & New Privacy Database **

The Centers for Medicare & Medicaid (CMS) reportedly has received more than 500,000 applications requesting an extension to the Oct. 15 transactions and code sets (TCS) compliance deadline by one year. At the same time, it was announced that CMS would be responsible for enforcing the HIPAA TCS standards. CMS and OCR, charged with enforcing the Privacy Rule, will work together on outreach and enforcement and on issues that touch both organizations.

Only a week earlier, CMS announced its plans to implement an electronic record management system as part of its compliance with the HIPAA medical privacy rule and the Privacy Act of 1974. The system, called the Privacy Accountability Database, will track access to CMS' health care data on more than 74 million Americans.

** Court Ruling Limits Prosecutors' Access to Patient Records **

New York State's highest court ruled last week that prosecutors cannot demand hospital medical records in their efforts to seek criminal suspects who have been wounded, because doing so infringes on patient confidentiality. The decision affects only cases that involve a doctor's medical judgment. Where information about a possible crime is apparent to anyone prosecutors may enforce a subpoena for records, the court noted in its unanimous decision.

Read more: http://www.hipaadvisory.com/news/index.cfm#1017nyt

** FTC: Pharmacies' Drug Marketing Violate Consumer Privacy? **

The Federal Trade Commission (FTC) has launched an investigation to determine whether pharmacies, including Walgreens and Rite-Aid, "improperly" use their customer lists to distribute promotional drug information paid for by pharmaceutical companies, the Wall Street Journal reports. The probe, which is in a "preliminary stage," is considering if the marketing practices violate federal false-advertising and medical privacy rules.

Read more: http://www.hipaadvisory.com/news/index.cfm#1017kais

** Spate of Snipings Raises Issues of Patient Privacy and Public Security **

The Washington Post reported last week on how a DC area hospital protected the identity of a 13-year-old high-profile patient. The boy, one of four wounded so far in the sniper attacks that

have left nine others dead since October 2, was admitted to Children's Hospital as a victim of violence. For his protection, he was assigned an alias, which became the name all staffers would use, and which anyone seeking information about him would have to know. A bogus file was created in the computer system to throw potential hackers off the trail.

Meanwhile Montgomery County, MD officials said it is too early to know what long-term changes could be made to improve public security, such as lobbying for a new national fingerprint database.

Read more: http://www.hipaadvisory.com/news/index.cfm#1017wp

==========

==========

3 >> H I P A A c t i o n: Feature Article

** Employee Health Benefit Plans: The Forgotten Covered Entity **

By William A. MacBain and Lisa B. MacBain
MacBain & MacBain, LLC

Organizations across the nation are working overtime to determine their HIPAA liability and to quickly remediate with appropriate changes in behavior and documentation. In the midst of all of this activity, it must be remembered that Federal HIPAA administrative simplification regulations treat employee health benefits plans as separate legal entities, distinct from their employer sponsors. Depending on how these health plans provide their benefits, they may be subject to some, or all, of the administrative simplification regulations.

Eligibility Considerations

Under the HIPAA privacy regulations, an employee health benefit plan and the employer, as plan sponsor, are considered separate legal entities. This is consistent with the treatment of employee welfare benefit plans under the Employee Retirement Income Security Act (ERISA). If the employee health benefit plan has 50 or more participants or if it is administered by a third party, it is considered a "group health plan" in the HIPAA regulations. If the employee health benefit plan meets this definition of a group health plan, it is considered a "covered entity" and is subject to HIPAA administrative simplification regulations. This includes regulations regarding standard transactions and codes sets, privacy, and security when the final security rules are published. A group health plan that provides all of its benefits through insurance contracts with health insurance companies or HMOs, does not need to comply with many of the administrative requirements of HIPAA, but it is still considered a covered entity and is subject to all other provisions of the regulations. However, if the group health plan provides any benefits on some

other basis, rather than through insurance contracts, it is subject to all of HIPAA, just as if it were a commercial insurance company.

Sharing Protected Health Information Between A Group Health Plan and Sponsor

Plan documents will need to be modified if any employees of the employer that sponsors the group health plan receive any protected health information (PHI) from the plan, other than eligibility verification and summary health information. This includes receiving protected health information from the group health plan's business associates, such as a TPA or pharmacy benefit manager. See 45 CFR A Â§ 164.504(f) Requirements for group health plans.

The relationship defined by HIPAA among the group health plan, the plan sponsor, a TPA, and other entities, can be confusing. When employees of the plan sponsor perform plan administration duties, their access to the group health plan's PHI is considered a disclosure of PHI from the group health plan to the plan sponsor. When employees of a TPA under contract to the group health plan have access to the group health plan's PHI, this is considered a disclosure of the PHI to the group health plan's business associate. Similarly, when plan administration is carried out by employees of the group health plan (example: Taft-Hartley trust), their access to PHI is a use of the group health plan's PHI. If the TPA's employees, or group health plan employees, provide PHI to the plan sponsor, this is also a disclosure of the PHI to the plan sponsor.

Disclosure of PHI to the plan sponsor is only allowed if the plan documents are amended. There are two exceptions: summary health information and enrollment information. Summary health information and enrollment information are PHI, but they may be disclosed to the plan sponsor even if the plan documents have not been amended. For HIPAA purposes, summary health information means information about individual participants in a group health plan that summarizes claims history, claims expenses, or type of claims experienced by those participants; and which has been de-identified, except that the information may be aggregated by 5-digit zip code instead of 3-digit zip code. Enrollment information is information determining whether an individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan to the plan sponsor.

Few organizations that sponsor a self-funded employee health plan can erect an impermeable barrier between the employer, as plan sponsor, and PHI in the custody of the group health plan - even if the plan is administered by a TPA. A careful review of information received from the TPA is recommended before concluding that the sponsor of a self-funded health plan can forego the HIPAA plan document amendments. This should include both routine reports and occasional information requests. Even in insured experience-rated plans, the plan sponsor may want to reserve the right to review high cost claims or other forms of PHI - and, thus, may want to amend the plan documents to allow these disclosures.

Amending Employee Welfare Benefit Plan Documents: Protecting the Privacy of Employee PHI When the Plan Sponsor is a Health Care Provider

HIPAA privacy regulations do not address the exchange of PHI between a group health plan and its plan sponsor, when the sponsor is also a covered health care provider, and the exchange is part of the normal commerce between a provider and a health plan.

For example, it would be normal for a health plan to send a remittance advice to a provider. However, if the provider is also the plan sponsor, and the health plan is the group health plan which the provider sponsors, a literal reading of the regulations would prohibit this practice. See 45 CFR Â§ 164.504(f)(2)(iii)(B). The rules regarding disclosures of PHI by a group health plan to its plan sponsor restrict the sponsor's access to and use of group health plan PHI, to only the

plan administration functions that the sponsor performs for the group health plan.

This literal reading would interfere with the ability of the sponsor, in its capacity as a provider, to receive PHI from its own group health plan for purposes related to its function as a provider.

One suggested approach is to treat such interactions under the same rules as apply to all other provider-health plan interactions, and to view this as something apart from the group health plan-plan sponsor relationship. This is consistent with the overall logic of the regulations, in the context of the entire administrative simplification section of HIPAA. However, readers are cautioned that this is an interpretation. This apparent conflict in the regulations points out the necessity for health care providers to use extra care in devising policies, procedures and training for workers who handle the PHI of fellow employees in the course of their duties.

Regardless of the approach taken, PHI will most likely need to be shared between employers, as plan sponsors, and those administering the employee health benefit plan. Compliance dates for documentation and training requirements are the same for all covered entities, including the employee health benefit plan. An exception is employee health benefit plans that paid less than $5 million in claims and insurance premiums in the most recent full fiscal year are considered small health plans, have an extra year to comply with the privacy regulations.

William and Lisa MacBain are principals of MacBain & MacBain, LLC, a health care consulting firm with particular expertise in the HIPAA regulations as they relate to managed care, hospital and health services, and employee benefit health plans.

==========

4 >> H I P A A / EDI: Q/A on Transactions & Code Sets

** The Addenda Are Coming! **

by Kepa Zubeldia, M.D., President/CEO of Claredi

QUESTION: Can you fill us in on the latest EDI transactions news? In particular, what is happening with the draft Addenda?

ANSWER: The X12 Healthcare Task Group met in Miami last week. The meeting was packed full, with extensive discussion about the HIPAA Addenda to the Implementation Guides, and with open forums for public discussion about the changes in the Addenda.

Finally, after a couple of Draft releases of the Addenda in October 2001 and August 2002, and extensive comments during the public comment period, the Addenda are ready for final publication. We are expecting final publication in October 2002 through the usual WPC-EDI web site: http://www.wpc-edi.com/hipaa/HIPAA_40.asp

The final version of the Addenda have small but important differences from previous drafts, that have come out of the NPRM comment period, the DSMO (Designated Standard Maintenance Organizations from the Transactions Final Rule) and the X12 comment periods. Of particular interest is the removal of the Taxonomy code (provider specialty) from most of the 837 Institutional Claim, a better definition of how to handle NDC codes in the claim, and the possibility to express anesthesia services in either minutes or units. There are changes to most other transactions too.

Now that the Addenda are final, the Secretary will be able to adopt them as part of the HIPAA standards. According to HHS representatives, we should expect the Final Rule adopting the Addenda around the end of 2002. And as soon as the Final Rule is published, the Medicare

Carriers and Intermediaries will receive instructions on how and when they must implement the Addenda. All the indications at this point are that the Addenda version of the HIPAA Implementation Guides will replace the current version of the guides published in May of 2000 before the end of the Administrative Simplification Compliance Act (ASCA) extension period.

What does this mean to you? If you have implemented the May 2000 version of the HIPAA guides, you will need to switch to the Addenda version by October 16, 2003. If you have implemented based on one of the previous Addenda drafts, you will have to make some adjustments to reflect the final Addenda version. But the changes should be easy.

Go forth and do good.

Kepa Zubeldia, M.D., is President and CEO of Claredi, a leading provider of HIPAA EDI compliance testing and certification.

==========

5 >> H I P A A / LAW: Legal Q/A

** HHS Responds to Frequently Asked Questions **

by Steve Fox, Esq., & Rachel Wilson, Esq., Pepper Hamilton LLP

On October 2nd, the Department of Health and Human Services ("HHS") posted responses to questions frequently asked about the HIPAA Privacy Rule (the "Rule"). The FAQs provide additional guidance about an individual's right to review his/her medical record, safeguards required when disclosing protected health information ("PHI"), incidental disclosures and the minimum necessary rule, and business associate requirements. The following is a brief summary of several of the more significant FAQs:

* PATIENTS' REVIEW OF THEIR MEDICAL RECORD. Who pays for the cost of copying medical records that patients request as permitted by the Rule?

Covered entities may impose reasonable fees for the cost of copying and postage. Fees must be based upon the actual production costs incurred by the entity, which would include the cost of labor, supplies, and postage; with the exception that costs associated with the search and retrieval of the requested information cannot be recovered from the patient. The covered entity may charge a fee for preparation of a summary or explanation of PHI, in those cases where a patient has agreed to receive such a summary or explanation in lieu of the actual records.

* SAFEGUARDS TO PROTECT PHI. Can covered entities transmit PHI via fax?

As long as the disclosure is permitted under the Rule, it can be made by fax or any other means. However, whatever the chosen means, it is subject to the reasonable and appropriate administrative, technical, and physical safeguards that covered entities are required to implement under the Rule (i.e., security considerations). An example of such safeguards would include requiring employees to confirm the fax number of the recipient prior to sending the fax, and making sure the fax machine is not accessible except to those that are authorized to use it.

* INCIDENTAL DISCLOSURES & THE MINIMUM NECESSARY RULE. Are patient sign-in sheets prohibited under the Rule? What about calling the names of patients in a waiting room?

Just to dispel any remaining uncertainty about this, HHS is telling us again that disclosures resulting from using sign-in sheets and calling-out for patients in waiting rooms are considered the incidental by-product of otherwise permissible disclosures related to treatment, payment,

and health care operations. Both practices are permissible, but only to the extent that reasonable and appropriate safeguards have been implemented to protect the privacy of PHI and limit the disclosure to the minimum amount necessary. For example, sign-in sheets should only require patients' names, not social security numbers, reason for visit, symptoms, or any other personal information which may be obtained privately. Similarly, displaying the names of patients next to the door of their hospital rooms and placing patient charts outside exam rooms are also permitted under the Rule subject to the same requirements.

* BUSINESS ASSOCIATES. Will physicians be considered the business associates of health plans or other payers? Are mail delivery personnel, plumbers, electricians, and other technicians and service providers the business associates of the covered entities to whom they provide service? Does HIPAA require covered entities to monitor business associate compliance with the Rule?

If the only relationship between a health plan and a provider is one where the provider submits claims for payment, then the provider is not a business associate of the health plan. Business associate relationships arise where a function or service is performed for or on behalf of a covered entity or where certain services are provided to a covered entity; PROVIDED, that the service or function involves the use or disclosure of PHI. That is generally not the case with providers and payers.

Plumbers, electricians and other technicians do not require access to PHI in order to perform their services. Therefore, they do not meet the definition of a business associate. Although mail delivery personnel may have access to PHI, they do not meet the definition of a business associate because they merely act as conduits to transport the information and no disclosure of PHI is intended. In all of these cases, it is possible that individuals performing these services may inadvertently see or have access to PHI. However, as long as the covered entity used reasonable and appropriate administrative, technical, and physical safeguards to minimize the chances for such exposure, no violation of the Rule will occur.

HHS again clarifies that although the Rule does not require covered entities to monitor, audit or oversee business associates for HIPAA compliance, it does require covered entities to enter into written business associate agreements in order to protect the privacy of patients' PHI. Furthermore, if a covered entity discovers material violations by its business associate, it must then immediately act to end the violation. If these attempts are unsuccessful, the business associate contract must be terminated. In the event that termination is not feasible, then the problem must be reported to HHS, Office of Civil Rights, the agency charged with administration and enforcement of the Rule. This area may well provide a fertile source for plaintiffs' attorneys, who will argue that the covered entity SHOULD have known of the business associate's violation, and was negligent for failing to prevent it or take action sooner.

For the full text of the FAQs, see:
http://www.hipaadvisory.com/action/faqs/faqs1001.doc

Read past HIPAA Legal Q/A articles:
http://www.hipaadvisory.com/action/LegalQA/archives.htm

Steve Fox, Esq., is a partner at the Washington, DC office of Pepper Hamilton LLP. This article was co-authored by Rachel H. Wilson, Esq., of Pepper Hamilton LLC. DISCLAIMER: This information is general in nature and should not be relied upon as legal advice.

==========

6 >> H I P A A / SECURE: Security Q/A

** Security Solutions: Key Technologies and Practices **
>> Encryption <<

by Eric Maiwald, CISSP

QUESTION: Can you explain a little about encryption and when we will need to use it?

ANSWER: Encryption is basically the hiding of information so that people who shouldn't see it, don't. Of course, that sounds simple but in practice it is a bit more difficult. When we talk about encryption we have two questions to answer: when do we use it and what do we use.

According to the draft security rule, encryption should be used when sensitive information traverses an open network. So now the question is what is an open network? It would appear to make sense to identify any network where the organization does not have control over the computers on the network as an open network. Therefore, the Internet would be an open network while the network inside the organization's data center is not (since the organization has control over the systems placed in the data center).

Based on this example, we would need to use encryption any time sensitive information is sent over the Internet. This might be when information is sent in emails, provided over a web page or sent in a file via FTP.

The type of encryption that you should use will depend on the way that the sensitive information is moving. For example, if you are sending information via email, you could use PGP (Pretty Good Privacy) to encryption the text of the email or use could use S/MIME to encode the email. There are also systems available that provide the sensitive content via a secure web (HTTPS) interface. If sensitive information is to be provided over the web, then a secure web site using Secure Socket Layer (SSL) should be provided. If the information is to be sent via FTP, you could encrypt the file before sending it or you used use SCP or SFTP to send the file.

All of the mechanisms I mentioned use some type of underlying encryption scheme or algorithm. In most cases, the choice of algorithm will be hidden from the user as it is embedded in the product or protocol that is used. As a general rule, it is best to use well-recognized protocols and encryption algorithms. This means that the protocol or algorithm has been examined to determine if backdoors or weaknesses exist. If this rule is followed, it is pretty unlikely that the information will be compromised by breaking the encryption. Please note that this does not mean that the information is completely protected. Most encrypted information is leaked by breaking the system surrounding the encryption. This means that the policy and procedures around the use of the encryption system are just as important, if not more so, than the algorithm that is chosen in the first place.

Eric Maiwald, CISSP, is Chief Technology Officer of Fortrex Technologies, which provides information security management, and process and monitoring services for healthcare organizations and other industries.

==========
7 >> H I P A A c t i o n: HIPAAwareness --

** Medical Practice "Before and After":
A HIPAA Reality Play in Two Acts **

by Helen Hadley, VantagePoint HealthCare Advisors

ACT I, SCENE I...BEFORE HIPAA

Typical busy physicians' office, early AM. Reception room is filled with patients. Ringing phones, conversations, and laughter emanate from the inner office.

(David, the receptionist, leans through open reception window, computer monitor in view, and a phone on his shoulder.)

DAVID. Good morning, Mrs. Adams. You are here for your colonoscopy, right? And, did you bring the oncologist's records?

MRS. ADAMS. Oh...uh, yes. I couldn't get my records, though. Can you have them faxed here?

(The medical assistant walks into the reception room.)

MEDICAL ASSISTANT. Mrs. Adams, we are ready for you. (She spots a familiar face and walks over.) Mrs. Flynn! How are you? I saw your daughter, Katie, the other day. She stopped in to pick up her lab test results before heading back to college. Is she OK?

MRS. FLYNN. (Puzzled and ruffled.) What do you mean? Katie was here for lab tests? She didn't say anything to me!

MEDICAL ASSISTANT. Oh, sorry, Mrs. Flynn. Maybe you can ask Dr. Trzaski. Mrs. Adams? Follow me...

SCENE II

(Exam Room #1. Mrs. Adams has just completed her visit with Dr. Matthews.)

MRS. ADAMS. Doctor, I am still unsure what is happening here. Can I please have a look at my records?

DR. MATTHEWS. Mrs. Adams, no need to worry yourself with paperwork...you know you can trust me. I will explain everything...

SCENE III

(Exam Room #2. Dr. Trzaski enters to find Mrs. Flynn flipping through her chart.)

DR. TRZASKI. Mrs. Flynn! (Surprised and annoyed.) May I have your record, please? If you have any questions, I will be happy to answer them for you.

MRS. FLYNN. Actually, Doctor, I do have questions about Katie. I understand that she had some lab tests performed. Can you tell me the results?

DR. TRZASKI. (Dials Medical Records.) Charlotte, please bring Katie Flynn's chart to me in Room 2.

SCENE IV

(Medical Records file room. Several file clerks are chatting, prepping charts, filing paperwork, and taking requests for chart pulls.)

REBECCA. Hey, Greg. Take a look at this chart. Isn't he in our class?

GREG. (Looking over Rebecca's shoulder.) You bet he is. Wait until everyone hears about this!

REBECCA. What should I do with these duplicate lab reports?

GREG. Just throw them out -- we only need one copy in the chart.

REBECCA. And, what about this records request from Attorney Anderson? What should I send?

GREG. Just photocopy the entire chart and get it out to her.

SCENE V

(Billing Office. Patient account representatives are working in an open office with billing records and charts strewn over desks.)

ALYSSA. (On the phone.) No, Mrs. Smith, we can't send your bill to your work address. We have only one field in the computer for an address. Sorry.

BRIAN. (On the phone.) You want us to change the diagnosis on your claim form? We can't do that! I understand that you didn't come in for your diabetes, but it IS one of your diagnoses, so there is no reason to change your record or claim form.

(The day is drawing to a close. Employees are rushing to finish their work. Tomorrow's charts are placed with the appointment schedule and left on the receptionist's desk. Wastebaskets overflow with discarded appointment schedules, superbills and duplicate reports. Filing cabinets are open, and billing office computer screens still reflect patient account information.)

ACT II, SCENE I...AFTER HIPAA

Same busy office, early morning.

(David, the receptionist, sits at the closed reception window, speaking quietly into a headset, and looks up at Mrs. Adams over the small flatscreen monitor that backs up to window area.)

DAVID. (Opening the window.) Good morning, Mrs. Adams. (He checks the appointment schedule to learn reason for Mrs. Adams' visit.) Did you bring along the records that we requested?

MRS. ADAMS. Hi...no, I couldn't get my records. Can you have them faxed here?

DAVID. Sure. In the meantime, this is our Privacy Notice. Please read it, and then I will need you to sign this Acknowledgement form so that we have a record of your receiving it.

(The medical assistant walks into the reception room.)

MEDICAL ASSISTANT. Mrs. Adams, we are ready for you. (She spots a familiar face and walks over.) Mrs. Flynn! How are you? How is Katie? Tell her I said 'hello.'

MRS. FLYNN. OK. But, I understand Katie was here for lab tests. Can you tell me anything?

MEDICAL ASSISTANT. Mrs. Flynn, I'm sorry, but you'll need to ask Katie for that information. We cannot release any information on patients without their authorization. I hope you understand. Mrs. Adams? Follow me...

SCENE II

(Exam Room #1. Mrs. Adams has just completed her visit with Dr. Matthews.)

MRS. ADAMS. Doctor, I am still unsure what is happening here. Can I please have a look at my records?

DR. MATTHEWS. Absolutely, Mrs. Adams, let me get one of our staff to show you to a private room to review your record.

SCENE III

(Exam Room #2. Dr. Trzaski opens the door to find Mrs. Flynn flipping through her chart.)

DR. TRZASKI. Hello, Mrs. Flynn! Did you have any questions regarding your records? I will be happy to answer them for you.

MRS. FLYNN. Actually, Doctor, I do have several questions about Katie. I understand that she had some lab tests last week. Can you tell me the results?

DR. TRZASKI. I understand your concern, Mrs. Flynn. However, if Katie is a patient here and she wants to share her information, she will have to provide us with a written authorization.

SCENE IV

(Medical Records file room. Several file clerks are chatting, prepping charts, filing paperwork, and taking requests for chart pulls.)

REBECCA. Hey, Greg. Take a look at this chart. Isn't he in our class?

GREG. Rebecca, you know we shouldn't be discussing any patient or looking at their records. Please, just file the lab work and put the chart back in file.

REBECCA. What should I do with these duplicate lab reports?

GREG. Shred the duplicates. We need only one copy in the chart.

REBECCA. And, what about this request for records from Attorney Anderson? What should I send out?

GREG. Our Privacy Officer should review these record requests. She will decide if the appropriate authorization is in place and what should be sent. It might only be a portion of the entire record that will be released.

SCENE V

(Billing Office. Patient account representatives are working in an open office with billing records and charts strewn over desks.)

ALYSSA. (On the phone.) Certainly, Mrs. Smith, we can send your bill to your work address. May I take that information now?

BRIAN. (On the phone.) You want us to change the diagnosis on your claim form? Let me have my supervisor check with the physician and determine if we billed incorrectly. May I fax over to you or mail to you a "Request for Amendment" form? This will be the best way to get this corrected for you.

SCENE VI

(The day is drawing to a close. Employees are rushing to finish their work. Tomorrow's charts are placed with the appointment schedule in a lower closed file cabinet. The wastebaskets are overflowing with shredded, discarded papers. The filing cabinets are closed and computers are shut down.)

Helen Hadley, President of VantagePoint HealthCare Advisors, has 30+ years experience in medical practice management, with a recent focus on HIPAA compliance. VantagePoint assists medical group practices with reimbursement, operations and compliance issues.

==========

http://www.hipaadvisory.com/alert/archives.htm
==========